# СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ МЕХАНИЗМЫ РЕАЛИЗАЦИИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В ВОИНСКИХ КОЛЛЕКТИВАХ: АНАЛИЗ УЯЗВИМОСТЕЙ

# SOCIAL AND PSYCHOLOGICAL MECHANISMS FOR IMPLEMENTING SOCIAL ENGINEERING IN MILITARY COLLECTIVES: ANALYSIS OF VULNERABILITIES

УДК 159.98

**КЛЕЩЕВА Юлия Алексеевна**

**KLESHCHEVA Yulia Alekseevna**

***Аннотация.*** *В статье рассматриваются социально-психологические механизмы, лежащие в основе реализации социальной инженерии в воинских коллективах. Актуальность исследования обусловлена возрастанием*

*информационно-психологических угроз в условиях современных вооруженных конфликтов, где военнослужащие становятся ключевой мишенью манипулятивного воздействия. На основе анализа научной литературы выделены и систематизированы основные уязвимости воинской среды, делающие личный состав восприимчивым к социально-инженерным атакам. Особое внимание уделено таким механизмам, как авторитет субординации, групповая идентичность, социальное доказательство и дефицит информации. Предложены направления психологической контрподготовки военнослужащих.*

***Ключевые слова:*** *социальная инженерия; воинский коллектив; социально-психологические механизмы; уязвимости; информационно-психологическая безопасность; манипуляция сознанием; психологическая контрподготовка; человеческий фактор; военная психология; социальное влияние.*

***Abstract:*** *This article examines the socio-psychological mechanisms underlying the implementation of social engineering in military units. The relevance of the study stems from the increasing information and psychological threats in modern armed conflicts, where military personnel become key targets for manipulative influence. Based on an analysis of the scientific literature, the key vulnerabilities of the military environment that make personnel susceptible to social engineering attacks are identified and systematized. Particular attention is paid to mechanisms such as subordination authority, group identity, social proof, and information deficit. Directions for psychological counter-preparation of military personnel are proposed.*

***Keywords:*** *social engineering; military team; socio-psychological mechanisms; vulnerabilities; information-psychological security; manipulation of consciousness; psychological counter-preparation; human factor; military psychology; social influence.*

Современные вооруженные конфликты все в большей степени приобретают гибридный характер, в котором наряду с традиционными военными средствами активно используются методы информационно-психологического воздействия на личный состав войск. Как отмечает Д.Б. Икрамов, в условиях расширения арсенала средств, сил и методов ведения вооруженного противоборства одним из главных его компонентов выступает информационная война, где главным объектом поражающего воздействия остается военный потенциал страны и ее военная мощь, а определяющим фактором их устойчивости является «действующий человек» [12, С. 10-11]. В этой связи особую актуальность приобретает изучение феномена социальной инженерии – технологии психологического манипулирования, направленной на использование человеческих слабостей и доверия для получения доступа к конфиденциальной информации или побуждения к определенным действиям.

В отличие от традиционного хакерства, социальная инженерия является мало- или нетехнологичной: она манипулирует характеристиками человеческой природы, эксплуатируя желание людей быть добрыми и отзывчивыми [8, С. 2]. Именно психологическая составляющая делает социальную инженерию столь опасной для любой организации, а в военной среде, где цена утечки информации или ошибочного действия особенно высока, проблема приобретает критическое значение.

Воинские коллективы представляют собой специфическую социальную среду, обладающую рядом особенностей, которые могут выступать как факторами боевой эффективности, так и уязвимостями для внешнего манипулятивного воздействия. Вертикаль власти, жесткая субординация, высокая степень доверия между сослуживцами и командирами, закрытость информации и ограниченность коммуникаций с внешним миром – эти характеристики, составляющие основу армейской организации, могут быть успешно использованы злоумышленниками, владеющими техниками социальной инженерии. Как показывают современные исследования, даже в

самых защищенных системах человеческий фактор остается наиболее уязвимым звеном в силу предсказуемости поведения и психологических особенностей человека [7, С. 2].

Целью настоящей статьи является выявление и анализ социально-психологических механизмов реализации социальной инженерии в воинских коллективах, а также систематизация основных уязвимостей военнослужащих к данному виду манипулятивного воздействия. Задачи исследования включают: 1) анализ теоретических подходов к пониманию социальной инженерии как психологического феномена; 2) выделение ключевых механизмов влияния, используемых в социально-инженерных атаках на военнослужащих; 3) систематизацию индивидуально-психологических и социально-психологических уязвимостей воинской среды; 4) формулирование практических рекомендаций по повышению психологической устойчивости личного состава.

В научной литературе понятие «социальная инженерия» традиционно рассматривается в рамках двух основных подходов. Первый, более широкий, восходит к работам К. Поппера и понимает социальную инженерию как деятельность по целенаправленному преобразованию социальных институтов и отношений. Второй, более узкий и актуальный для целей настоящего исследования, трактует социальную инженерию как совокупность методов психологического манипулирования, направленных на получение доступа к информации или побуждение человека к действиям вопреки его интересам [7, С. 3]. Именно в этом значении термин используется в современной психологии информационной безопасности.

Ключевой особенностью социальной инженерии является опора на фундаментальные социально-психологические механизмы, детально описанные в работах Р. Чалдини. Как показывают исследования, большинство социально-инженерных атак строятся на принципах авторитета, взаимного обмена, социального доказательства, обязательства и последовательности, дефицита, симпатии [7, С. 2]. Эти механизмы, в обычных условиях

обеспечивающие эффективность социального взаимодействия и адаптацию человека к групповой жизни, в условиях целенаправленного манипулятивного воздействия превращаются в уязвимости.

В военной психологии проблематика социальной инженерии долгое время оставалась на периферии научных исследований, уступая место традиционным темам боевого стресса, лидерства и групповой сплоченности. Однако практика последних десятилетий, включая опыт участия российских Вооруженных Сил в вооруженных конфликтах за пределами страны, убедительно демонстрирует необходимость изучения социально-психологических аспектов информационного противоборства [12, С. 12]. Военные социологи и психологи, осуществляющие научное сопровождение деятельности армии непосредственно в боевой обстановке, все чаще сталкиваются с необходимостью оценки не только морально-психологического состояния личного состава, но и его уязвимости к внешним манипулятивным воздействиям.

Специфика воинского коллектива как объекта социально-инженерных атак определяется рядом факторов. Во-первых, это высокая степень институционализации и формализации отношений, где приказ вышестоящего начальника воспринимается как безусловный к исполнению. Во-вторых, это закрытость коммуникативных потоков: военнослужащие, особенно в условиях выполнения боевых задач, имеют ограниченный доступ к альтернативным источникам информации, что делает их более восприимчивыми к любой поступающей извне информации, особенно если она подается от имени официальных структур. В-третьих, это высокий уровень групповой идентичности и сплоченности, который, с одной стороны, является основой боеспособности, а с другой – создает предпосылки для феномена группового мышления и конформного поведения [5, С. 2].

В результате анализа научной литературы и эмпирических исследований в области противодействия социальной инженерии в Вооруженных Силах [8; 9; 11] было выделено девять ключевых факторов, влияющих на

восприимчивость военнослужащих к данному виду атак. Эти факторы могут быть рассмотрены как основные психологические механизмы, лежащие в основе реализации социальной инженерии в воинской среде.

Авторитет является, пожалуй, наиболее значимым механизмом в контексте воинского коллектива. Иерархическая структура военной организации предполагает безусловное подчинение младших по званию старшим. Злоумышленник, выступающий от имени вышестоящего командира или инспектора, может успешно использовать этот механизм для получения конфиденциальной информации или побуждения к действиям, выходящим за рамки служебных обязанностей. Эксперименты, проведенные исследователями при поддержке НАТО, показали, что использование поддельных аккаунтов в социальных сетях, имитирующих профили старших офицеров, позволяет эффективно влиять на поведение военнослужащих и склонять их к разглашению служебной информации.

Взаимный обмен (реципрокность) – механизм, основанный на стремлении человека ответить добром на добро. В воинской среде этот механизм может проявляться в ситуациях, когда злоумышленник сначала оказывает небольшую услугу (делится информацией, помогает с решением бытовой проблемы), а затем запрашивает в ответ конфиденциальные сведения. Как отмечают специалисты, социальные инженеры часто используют желание людей быть добрыми и отзывчивыми, что в условиях воинского коллектива, где взаимопомощь является нормой, приобретает особую силу [8, С. 3].

Обязательство и последовательность опираются на стремление человека выглядеть последовательным в своих действиях и поступках. Если военнослужащий однажды совершил незначительное действие в пользу злоумышленника (например, ответил на безобидный вопрос), то он с большей вероятностью согласится на более серьезные уступки, чтобы сохранить внутреннюю согласованность своего поведения.

Диффузия ответственности – феномен, хорошо известный в социальной психологии, заключается в снижении чувства личной ответственности в

присутствии других людей. В воинском коллективе, где многие действия регламентированы и осуществляются по приказу, диффузия ответственности может способствовать тому, что военнослужащий передает конфиденциальную информацию, полагая, что за это несут ответственность другие.

Дефицит – механизм, создающий искусственную ограниченность ресурса (времени, информации, доступа). Злоумышленник может убедить военнослужащего в том, что конфиденциальные сведения необходимо передать немедленно, иначе будет упущена уникальная возможность. В условиях дефицита времени, характерного для боевой обстановки, критическое мышление отключается, и человек действует по привычным алгоритмам.

Симпатия и благорасположение используют естественное стремление человека соглашаться с теми, кто ему приятен. Злоумышленники могут налаживать дружеские отношения с военнослужащими через социальные сети, общие интересы или создание искусственной общности.

Социальное доказательство – механизм, основанный на тенденции ориентироваться на поведение других людей в неопределенных ситуациях. Если военнослужащий видит, что его сослуживцы (или те, кого он принимает за сослуживцев) делятся информацией или совершают определенные действия, он с высокой вероятностью последует их примеру.

Осведомленность как фактор может выступать как в роли уязвимости, так и в роли защитного ресурса. Недостаток знаний о методах социальной инженерии и типовых сценариях атак делает военнослужащего легкой мишенью. И наоборот, целенаправленное информирование личного состава о рисках существенно повышает психологическую устойчивость [8, С. 4].

Доверие является ключевой характеристикой воинского коллектива. Высокий уровень доверия между сослуживцами и к командованию – основа боеспособности, но именно это доверие может быть использовано злоумышленниками, которые выдают себя за «своих».

Практические исследования подтверждают высокую эффективность использования данных механизмов в военной среде. Так, в ходе эксперимента, проведенного исследовательской группой при поддержке НАТО, с использованием поддельных аккаунтов в Facebook и Instagram (ресурсы признаны экстремистскими и запрещены) удалось не только собрать информацию о дислокации подразделений и передвижении войск, но и побудить военнослужащих к нежелательному поведению, включая оставление постов. Важно отметить, что бюджет эксперимента составил всего 60 долларов США, что демонстрирует крайне низкую стоимость и высокую эффективность социально-инженерных атак по сравнению с традиционными методами ведения разведки.

Анализ уязвимостей воинского коллектива к социальной инженерии предполагает рассмотрение данного феномена на трех уровнях: индивидуально-психологическом, социально-психологическом и организационно-процедурном.

На индивидуально-психологическом уровне ключевыми уязвимостями выступают:

- склонность к ригидности мышления, характерная для военнослужащих, длительное время находящихся в жестко регламентированной среде. Ригидность затрудняет критическую оценку нестандартных ситуаций и сценариев, что может быть использовано злоумышленниками;

- высокий уровень доверия к командованию и официальным инстанциям. Как показывают исследования, военнослужащие в силу профессиональной социализации склонны воспринимать любые указания, исходящие от лица, обладающего признаками власти, как обязательные к исполнению [5, С. 3];

- эмоциональное выгорание и накопленная усталость, особенно актуальные для военнослужащих, выполняющих боевые задачи в

экстремальных условиях. В состоянии усталости снижается критичность мышления и повышается восприимчивость к манипулятивным воздействиям;

- ротация личного состава и частая смена мест дислокации, ведущие к ослаблению горизонтальных социальных связей и снижению уровня взаимного контроля.

На социально-психологическом уровне выделяются следующие уязвимости:

- групповая сплоченность, которая при определенных условиях может трансформироваться в феномен группового мышления, когда критическая оценка информации приносится в жертву групповому консенсусу. Как отмечают исследователи, социальная сплоченность играет решающую роль на поле боя, но она же может быть использована для манипуляции [5, С. 4];

- круговая порука и неформальные нормы поведения, существующие в воинских коллективах. Злоумышленник, владеющий информацией об этих нормах, может эффективно имитировать поведение «своего»;

- боязнь нарушить единоначалие и иерархическую вертикаль, что препятствует инициативной проверке подозрительных запросов. Военнослужащий может опасаться беспокоить командира по «мелкому» вопросу и принять решение самостоятельно, в пользу злоумышленника;

- изолированность коллектива от внешней информации и альтернативных источников, что создает информационный вакуум, заполняемый любыми доступными данными, в том числе дезинформацией.

На организационно-процедурном уровне уязвимости связаны с:

- регламентированностью и стандартизацией коммуникаций. В военной среде многие коммуникации осуществляются по формализованным шаблонам, что облегчает подделку сообщений;

- приоритетом приказа и оперативности исполнения над критическим осмыслением. В боевой обстановке промедление может стоить жизни, поэтому военнослужащие приучены действовать быстро, не подвергая сомнению поступающие указания;

- недостаточной психологической контрподготовкой и отсутствием регулярного информирования о методах социальной инженерии. Как справедливо отмечают исследователи, проблема подготовки кадров занимает одно из первых мест в угрозах информационной безопасности, а обучение персонала распознаванию социально-инженерных атак является ключевым элементом противодействия [7, С. 4].

Особого внимания заслуживает феномен «социальной инженерии в закрытых коммуникативных потоках». А.А. Головинский в своем исследовании социальной психики военнослужащих обращает внимание на то, что замкнутость информационных каналов в воинской среде создает особые условия для формирования коллективных представлений и установок [2, С. 5]. Злоумышленник, сумевший внедриться в эти закрытые коммуникативные потоки или создать их имитацию, получает мощнейший рычаг воздействия на психику военнослужащих.

Практика участия российских Вооруженных Сил в вооруженных конфликтах показывает, что своевременное выявление и анализ уязвимостей личного состава к социально-инженерным атакам должны стать неотъемлемой частью социологического и психологического сопровождения деятельности войск. Как отмечается в работах по военной социологии, мониторинг морально-политического и психологического состояния военнослужащих, их готовности к выполнению боевых задач, а также изучение общественного мнения и настроений в воинских коллективах позволяют не только оценить текущее состояние, но и прогнозировать зоны повышенной уязвимости [12, С. 11].

На основе проведенного анализа могут быть предложены следующие направления психологической контрподготовки военнослужащих к социально-инженерным атакам.

Во-первых, необходимо внедрение регулярных информационно-психологических тренингов, направленных на формирование у личного состава «иммунитета» к манипулятивным воздействиям. Такие тренинги

должны включать ознакомление с типовыми сценариями социально-инженерных атак, разбор реальных кейсов (в том числе из практики участия российских Вооруженных Сил в боевых действиях), а также отработку навыков критической оценки нестандартных запросов и ситуаций.

Во-вторых, целесообразна разработка и внедрение процедур верификации подозрительных запросов, особенно тех, которые связаны с передачей конфиденциальной информации или побуждением к действиям, выходящим за рамки служебных обязанностей. Такие процедуры должны стать стандартом служебного поведения и не восприниматься как проявление недоверия или излишней подозрительности.

В-третьих, необходимо налаживание системы регулярного информирования военнослужащих о новых методах и сценариях социальной инженерии. Учитывая стремительное развитие технологий и появление все более изощренных атак (включая использование deepfake-технологий для имитации голоса и внешности командиров), информирование должно быть непрерывным и оперативным.

В-четвертых, важным направлением является психологическая работа с командирами всех уровней. Именно командиры, обладающие авторитетом в глазах подчиненных, могут стать как ключевой мишенью для злоумышленников (компрометация командира – эффективный способ воздействия на весь коллектив), так и основным ресурсом профилактики. Командиры должны быть обучены распознавать признаки социально-инженерных атак и транслировать подчиненным образцы бдительного поведения.

В-пятых, целесообразно включение тематики противодействия социальной инженерии в программы морально-психологической подготовки и боевого информирования. Как показывает опыт, информация о том, что большинство военнослужащих готовы к выполнению боевых задач и уверены в своих сослуживцах, оказывает позитивное влияние на моральный дух войск [12, С. 13]. Аналогичным образом, информация о существующих угрозах и

способах защиты должна стать частью повседневной информационной среды воинского коллектива.

Социальная инженерия представляет собой серьезную угрозу информационно-психологической безопасности воинских коллективов, эффективно использующую фундаментальные социально-психологические механизмы человеческого поведения. В основе реализации социально-инженерных атак на военнослужащих лежат такие механизмы, как авторитет, взаимный обмен, обязательство и последовательность, диффузия ответственности, дефицит, симпатия, социальное доказательство и доверие. Воинская среда в силу своей специфики (вертикаль власти, высокая степень доверия, закрытость коммуникаций, приоритет оперативности исполнения) создает благоприятные условия для использования этих механизмов злоумышленниками.

Анализ уязвимостей на индивидуально-психологическом, социально-психологическом и организационно-процедурном уровнях позволяет выделить ключевые направления повышения психологической устойчивости личного состава. Наиболее эффективными мерами противодействия выступают регулярное информирование военнослужащих о методах социальной инженерии, внедрение процедур верификации подозрительных запросов, психологическая работа с командирами всех уровней, а также включение соответствующей тематики в программы боевой и морально-психологической подготовки.

Дальнейшие исследования в данной области должны быть направлены на эмпирическую верификацию выделенных механизмов и уязвимостей в различных категориях военнослужащих, разработку валидных методик диагностики подверженности социально-инженерным атакам, а также создание комплексных программ психологической контрподготовки с учетом специфики конкретных воинских специальностей и условий выполнения боевых задач.

## СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ:


1. Барановский М.В. Социологическое сопровождение деятельности военной организации в боевых условиях // Мониторинг правоприменения. 2021. № 1 (38). С. 46-50.
2. Головинский А.А. Изменение иерархии доминирующих ценностей личности как результат ведения ментальной войны // Вестник адъюнкта. 2021. №4. [Электронный ресурс]. URL: http://vestnik-adyunkta.ru (дата обращения: 12.05.2024).
3. Дубинин И.В. Факторы управляемости воинскими подразделениями Вооруженных Сил Российской Федерации // Психологические науки. 2023. № 1. С. 24-31.
4. Икрамов Д.Б. Системно-коммуникационные аспекты военно-социологического подхода к оценке информационно-психологической безопасности военнослужащих // Коммуникология. 2022. Т. 10. № 4. С. 94-105.
5. Икрамов Д.Б. Проблемы совершенствования системы социологического обеспечения управленческой деятельности Вооруженных Сил Российской Федерации в условиях активизации информационно-психологических угроз // Вопросы безопасности. 2020. № 3. С. 10-18.
6. Пителинский К.В., Гончаренко Г.Ю., Ермаков И.К., Ермолатий Д.А. Компьютерная психология или универсальный подход к уязвимостям конфиденциальной информации // Вопросы защиты информации. 2018. № 4. С. 62-68.
7. Чалдини Р. Психология влияния. СПб.: Питер, 2020. 416 с.
8. Шиллер Г. Манипуляторы сознанием. М.: Мысль, 1980. 326 с.
9. Яковлев В.И. Технологии манипулирования сознанием военнослужащих в контексте решения задач информационно-психологического противоборства. М.: ВУ, 2015. 180 с.

10. Fabrigar L.R. The psychology of non-kinetic activities by military forces: a review of themes, implications, and unresolved issues in the study of attitudes, persuasion, and social influence. Kingston: Queen‘s University, 2018. 245 p.
11. Hagan K.R. The six pillars of influence: how insurgent organizations manipulate governments, populations, and their operatives. Monterey: Naval Postgraduate School, 2009. 112 p.
12. Shahrom M.F., Maarop N., Samy G.N., Hassan N.H., Abdul Rahim F., Magalingam P., Kamaruddin N. A pilot analysis of factors affecting defense against social engineering attacks in the armed forces environment // Open International Journal of Informatics. 2021. Vol. 9. No. 1. Pp. 53-64.

**REFERENCES:**

1. Baranovsky M.V. Sociological Support of the Activities of a Military Organization in Combat Conditions // Monitoring of Law Enforcement. 2021. No. 1 (38). Pp. 46-50.
2. Golovinsky A.A. Change in the hierarchy of dominant values of the personality as a result of conducting the mental war // Adjunkt’s Bulletin. 2021. №4. [Electronic resource]. URL: http://vestnik-adyunkta.ru (Access date: 12.05.2024).
3. Dubinin I.V. Factors of Controllability of Military Units of the Armed Forces of the Russian Federation // Psychological Sciences. 2023. No. 1. Pp. 24-31.
4. Ikramov D.B. Systemic and communication aspects of the military-sociological approach to assessing the information and psychological security of military personnel // Communicology. 2022. Vol. 10. No. 4. Pp. 94-105.
5. Ikramov D.B. Problems of improving the system of sociological support for the management activities of the Armed Forces of the Russian Federation in the context of intensifying information and psychological threats // Security Issues. 2020. No. 3. Pp. 10-18.

6. Pitelinsky K.V., Goncharenko G.Yu., Ermakov I.K., Ermolatiy D.A. Computer psychology or a universal approach to the vulnerabilities of confidential information // Information Security Issues. 2018. No. 4. Pp. 62-68.
7. Cialdini R. Psychology of influence. St. Petersburg: Piter, 2020. 416 p.
8. Schiller G. Manipulators of Consciousness. Moscow: Mysl', 1980. 326 p.
9. Yakovlev V.I. Technologies for Manipulating the Consciousness of Military Personnel in the Context of Solving Information-Psychological Confrontation Problems. Moscow: VU, 2015. 180 p.
10. Fabrigar L.R, The Psychology of Non-Kinetic Activities by Military Forces: A Review of Themes, Implications, and Unresolved Issues in the Study of Attitudes, Persuasion, and Social Influence. Kingston: Queen's University, 2018. 245 p.
11. Hagan K.R. The Six Pillars of Influence: How Insurgent Organizations Manipulate Governments, Populations, and Their Operatives. Monterey: Naval Postgraduate School, 2009. 112 p.
12. Shahrom M.F., Maarop N., Samy G.N., Hassan N.H., Abdul Rahim F., Magalingam P., Kamaruddin N. A pilot analysis of factors affecting defense against social engineering attacks in the armed forces environment // Open International Journal of Informatics. 2021. Vol. 9.No. 1. Pp. 53-64.

**Клещева Юлия Алексеевна**
соискатель кафедры социологии
Военный университет имени князя Александра Невского
123001, г. Москва, Б. Садовая ул., д. 14, стр. 1.
julliaand@yandex.ru

**Kleshcheva Yulia Alekseevna**
Applicant for a degree at the Department of Sociology
Military University named after Prince Alexander Nevsky
B. Sadovaya ul., d.14, building 1, Moscow, Russia, 123001

5.3.3. Психология труда, инженерная психология, когнитивная эргономика.